

Quirky Quantifiers: Optimal Models and Complexity of Computation Tree Logic

Martin Lück

Institut für Theoretische Informatik
Leibniz Universität Hannover, DE
lueck@thi.uni-hannover.de

Abstract

The satisfiability problem of the branching time logic CTL is studied in terms of computational complexity. Tight upper and lower bounds are provided for each temporal operator fragment. In parallel the minimal model size is studied with a suitable notion of minimality. Thirdly, flat CTL is investigated, i.e., formulas with very low temporal operator nesting depth. A sharp dichotomy is shown in terms of complexity and optimal models: Temporal depth one has low expressive power, while temporal depth two is equivalent to full CTL.

1 Introduction

Background. In the last decades temporal logics have successfully established as a well-known framework for verification of dynamic, reactive systems. The first one who systematically introduced time into modern logic was Arthur Prior who used modal logic as a base framework [Pri57]. The resulting system was called *tense logic*. Amir Pnueli discovered the usefulness of such logics for formally describing the behavior of dynamic systems with discrete time steps [Pnu77]. His suggested method of temporal reasoning on sequential and parallel programs developed to a broad family of logics; especially the linear time logic LTL, the branching time logic CTL and their extensions have remarkable importance in industrial verification. They have been researched thoroughly in terms of their expressivity as well as computational complexity. In particular, the tractable model checking problem of CTL allows large-scale applications in practice, while its satisfiability or equivalently validity problem is EXP-complete and therefore proven definitely intractable [FL79, Pra80, AE90].

Due to the highly infeasible nature of temporal logics, many of their *fragments* have been investigated, including restricted temporal operator sets, bounded operator nesting depth, bounded number of variables and restricted sets of logical connectives [SC85, Hal95, DS02, Sch02, MMTV09]. The results are not too optimistic: For no fragment of CTL or LTL the satisfiability problem becomes tractable, except for trivial combinations of Boolean connectives [MMTV09]. Restricting the CTL or LTL operators or the number of propositions does not decrease the computational complexity noteworthy; and also very low temporal depth already carries the complexity of LTL beyond tractability [SC85, DS02, Sch02].

In the converse this means that even “simple” and “flat” temporal formulas have sufficient expressive power, a fact that is reflected by their application in practice. Many important properties of computations like safety, deadlock-freeness/liveness or fairness are expressible in temporal depth two or three. Exceptions are CTL model checking, which is inherently sequential [Bey+09], but only at the price of unbounded temporal depth, and pure modal satisfiability as a sublogic of CTL, which drops down to NP for bounded depth but is otherwise PSPACE-complete even for only one proposition [Hal95].

The minimal model size of a formula, or generalized, of a class of formulas, can serve as an indicator for its expressive power. Minimal models are also useful to consider for



© Martin Lück;
licensed under Creative Commons License CC-BY

Leibniz International Proceedings in Informatics
LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

algorithms that proof satisfiability by searching a space of potential models, as then the size (resp. depth) of minimal models can deliver an upper bound for the required time (resp. memory) of the algorithm. For the investigated fragments of CTL the results range over exponentially deep models, big but shallow tree-like models down to polynomial models. A more or less direct translation into complexity classes of the satisfiability problem will be made.

Contribution. This paper continues the systematical study of temporal logic fragments. The considered fragments are sublogics of CTL obtained by limiting temporal operators, their nesting depth or both. For each resulting fragment, tight upper and lower bounds are established in terms of computational complexity. The notion of minimal models is introduced and upper and lower bounds are achieved, again as a complete classification of all fragments.

There are upper bounds in complexity which are corollaries from small minimal models (like the NP cases), but also several hardness results automatically yield formulas which require large models. Thus it may not be very surprising that the results in both dimensions closely correlate; specifically a temporal depth of two seems to be the “magical threshold” for the hardness of CTL, a behavior that can also be observed for LTL [DS02].

2 Preliminaries

The set of all atomic propositional statements p_1, p_2, \dots is denoted \mathcal{PS} . Boolean functions are for example \wedge (and) which can also be written as product (\cdot) , and \vee (or) which can also be written as sum $(+)$, and \neg (negation).

► **Definition 2.1** (Boolean clone). Let C be a set of Boolean functions. Then the *clone* $[C]$ is the smallest superset of C that is closed under composition and projections to arguments.

Important clones are $\text{BF} := [\{\wedge, \neg\}]$ and $\text{S}_1 := [\{\nrightarrow\}]$, where \nrightarrow is the negated Boolean implication (see [Pos41]). In the following C is used as set of Boolean functions as well as set of available function symbols, the *base* of the clone. For CTL formulas we use a similar notation as Allen Emerson, Halpern and Schnoebelen [AEH86, Sch02], but generalize to use different Boolean functions.

Write $T_1 \cdot T_2$ for $\{O_1 O_2 \mid O_1 \in T_1, O_2 \in T_2\}$.

► **Definition 2.2** (CTL syntax). The set $\text{TL} := \{A, E\} \cdot \{X, F, G, U, R\}$ is the *set of CTL operators*. For $Q \in \{A, E\}$, QX, QF, QG are *unary*, QU, QR are *binary*. Let C be a set of Boolean functions and $T \subseteq \text{TL}$. Define sets of CTL formulas as the smallest sets s.t. f.a. $i \geq 0$ holds:

$\mathcal{PS} \subseteq \mathcal{B}_i(T, C) \subseteq \mathcal{B}_{i+1}(T, C)$. If $\varphi \in \mathcal{B}_i(T, C)$, then $O\varphi \in \mathcal{B}_{i+1}(T, C)$ for a unary $O \in T$. If $\varphi, \psi \in \mathcal{B}_i(T, C)$, then $\varphi O \psi \in \mathcal{B}_{i+1}(T, C)$ for a binary $O \in T$. $\mathcal{B}_i(T, C) = \langle \mathcal{B}_i(T, C) \rangle_C$, where $\langle \cdot \rangle_C$ is the closure under syntactical composition using function symbols from C .

Usually we will omit T if $T = \text{TL}$ resp. C if $[C] = \text{BF}$, and use $C = \{\wedge, \vee, \neg\}$ writing $\alpha \rightarrow \beta$ for $\neg\alpha \vee \beta$ and so on. We omit brackets if the meaning is understood. Unary operators (\neg and temporal operators) take precedence before binary operators, \wedge before \vee , and \wedge, \vee before \rightarrow and \leftrightarrow .

With this notation, \mathcal{B} is the *set of syntactically valid CTL formulas*. If $T \subseteq \text{TL}$, then $\mathcal{B}(T)$ is an *operator fragment*. If $[C] \subseteq \text{BF}$, then $\mathcal{B}(C)$ is a *Boolean fragment*. The set \mathcal{B}_i is the fragment of CTL formulas with *temporal (nesting) depth* at most i , and \mathcal{B}_1 is the set of *flat* CTL formulas, i.e., every temporal operator contains only purely propositional formulas.

If the necessary Boolean functions are available, we refer to CTL operator fragments by a minimal defining set using these functions, using only A-quantified operators if possible, e.g., the fragment $\{AF, AU, EG, ER\}$ is equivalent to $\{AU\}$ via the symbols \neg and \top . More general we say that a set T of temporal operators can *define* an operator O in the clone $[C]$ if any formula $O\psi$ is equivalent to a formula using only operators resp. Boolean functions from $T \cup C$. Likewise, T can define O if it can define it for $[C] = BF$, and T can define a set $T' \subseteq TL$ (in $[C]$) if T' can define all $O \in T'$ (in $[C]$).

► **Definition 2.3** (Kripke structures). A *Kripke frame* is a tuple (W, R) where W is the set of *worlds* and $R \subseteq W \times W$ is the *successor* or *accessibility relation*. A Kripke frame is *serial* or *total* if R is total, i.e., every $w \in W$ has at least one R -successor.

A *Kripke structure* is a tuple $\mathcal{M} = (W, R, V)$ where (W, R) is a Kripke frame and $V: \mathcal{PS} \rightarrow \mathfrak{P}(W)$ is the *valuation function* which maps to each atomic proposition the subset of worlds in which the proposition holds.

► **Definition 2.4** (Paths). A *path* $\pi = (w_0, w_1, \dots)$ through a Kripke frame (W, R) is an infinite sequence of worlds $w_i \in W$ with $w_i R w_{i+1}$ f.a. $i \geq 0$. Write $\pi[i] := w_i$ and $\pi_{\geq i} := (w_i, w_{i+1}, \dots)$. Write $\Pi(w)$ for the set of all paths starting at w .

► **Definition 2.5** (CTL Semantics). In the following \mathcal{M} denotes a Kripke structure, w a world in \mathcal{M} , π a path through \mathcal{M} , f an n -ary Boolean function, θ a Boolean assignment to f and $[n] := \{1, \dots, n\}$. Define:

$$\begin{aligned}
(\mathcal{M}, w) \models x \quad \text{for } x \in \mathcal{PS} & \quad \text{iff } w \in V(x) \\
(\mathcal{M}, w) \models f(\varphi_1, \dots, \varphi_n) & \quad \text{iff } \exists \theta : \theta \models f \text{ and } \forall i \in [n] : \theta(i) = 1 \Leftrightarrow (\mathcal{M}, w) \models \varphi_i \\
(\mathcal{M}, w) \models A\psi & \quad \text{iff } \forall \pi \in \Pi(w) : (\mathcal{M}, \pi) \models \psi \\
\\
(\mathcal{M}, \pi) \models x \quad \text{for } x \in \mathcal{PS} & \quad \text{iff } \pi[0] \in V(x) \\
(\mathcal{M}, \pi) \models f(\varphi_1, \dots, \varphi_n) & \quad \text{iff } \exists \theta : \theta \models f \text{ and } \forall i \in [n] : \theta(i) = 1 \Leftrightarrow (\mathcal{M}, \pi) \models \varphi_i \\
(\mathcal{M}, \pi) \models A\psi & \quad \text{iff } (\mathcal{M}, \pi[0]) \models A\psi \\
(\mathcal{M}, \pi) \models X\psi & \quad \text{iff } (\mathcal{M}, \pi_{\geq 1}) \models \psi \\
(\mathcal{M}, \pi) \models \psi U \psi' & \quad \text{iff } \exists i \geq 0 : (\mathcal{M}, \pi_{\geq i}) \models \psi' \\
& \quad \text{and } \forall j < i : (\mathcal{M}, \pi_{\geq j}) \models \psi
\end{aligned}$$

From the point of semantics, interpret the remaining symbols as $E \hat{=} \neg A \neg$, $F \hat{=} \top U$, $G \hat{=} \neg F \neg$ and $\alpha R \beta \hat{=} \neg[\neg \alpha U \neg \beta]$.

If the model \mathcal{M} is clear from the context, also write $w \models \varphi$ or $\pi \models \varphi$ instead of $(\mathcal{M}, w) \models \varphi$ and $(\mathcal{M}, \pi) \models \varphi$.

► **Definition 2.6** (Satisfiability). The set $SAT(\Gamma)$ for $\Gamma \subseteq \mathcal{B}$ contains all *satisfiable* formulas $\varphi \in \Gamma$, i.e., for which there is a serial Kripke structure \mathcal{M} with root w s.t. $(\mathcal{M}, w) \models \varphi$.

If no root is given explicitly, then it is clear from the context, for instance because there is only one world in \mathcal{M} without predecessors.

► **Definition 2.7** (Formula and structure size and depth). The size $|\varphi|$ of $\varphi \in \mathcal{B}(TL)$ is the total number of propositions, Boolean connectives and temporal operators in φ .

A Kripke model $\mathcal{M} = (W, R, V)$ with root $w \in W$ is *R-generable* if every world $w' \in W$ is reachable from w through an R -path.

The size $|\mathcal{M}|$ of a Kripke model $\mathcal{M} = (W, R, V)$ is the total number $|W|$ of worlds in \mathcal{M} . The depth $d(\mathcal{M})$ of an R -generable Kripke model is the maximum depth of a world $w \in W$, where the depth of a world is the maximum length of a simple¹ R -path from the root to w .

The definition of size differs from the binary encoding size in which the propositions would require $\log n$ bits. But this factor can be neglected both for the results about optimal models (as models would have the same encoding overhead) and with regard to the involved complexity classes. We further assume all satisfying Kripke models as R -generable without loss of generality.

Note that the usual definition of depth is via shortest paths, not longest. But this would not be very interesting for some operators like **AG** for which its formulas can always be fulfilled on transitive structures where all shortest paths have length one. Instead we want to know how long the simple paths in a model must be before ending in back-edges. If the model cannot be assumed both shallow and tree-like, then this measure is more suitable for indicating the memory requirement for satisfiability testing.

► **Definition 2.8** (Optimal model size and depth). Let $\Gamma \subseteq \mathcal{B}$ be a set of temporal formulas. Then the *optimal model size* $\sigma(\Gamma): \mathbb{N} \rightarrow \mathbb{N}$ is the function that maps each $n \in \mathbb{N}$ to the expression

$$\max \{ \min \{ |\mathcal{M}| : \mathcal{M} \models \varphi \} : \varphi \in \text{SAT}(\Gamma), |\varphi| = n \}.$$

In other words, if $\sigma(n) = m$ then all satisfiable formulas of size n have a model of size m , but not all formulas of size n have a model of size $< m$.

Similar define the *optimal model depth* $\delta(\Gamma)$ with the depth $d(\mathcal{M})$ instead of the size.

► **Theorem 2.9** (Small model property of CTL [AE90]). \mathcal{B} has optimal model size of at most $2^{\mathcal{O}(n)}$.

► **Theorem 2.10** ([FL79, Pra80, AE90]). $\text{SAT}(\mathcal{B})$ is \leq_m^P -complete for **EXP**.

3 Restricted sets of CTL operators

In this section for every operator fragment the upper bounds are either improved, or proven tight. We begin with proving the lower bounds for the fragment $\mathcal{B}(\text{AF})$.

3.1 The AF fragment

For the lower bound in computational complexity we consider a reduction from the PSPACE-complete problem of *quantified Boolean formulas* (qbfs). We start with the following lemmas.

► **Lemma 3.1.** Let $\psi = Q_1 x_1 \dots Q_n x_n H$ be a qbf. It holds that $\psi \equiv \top$ if and only if $Q_1 \ell_1 \in \{x_1, \neg x_1\} \dots Q_n \ell_n \in \{x_n, \neg x_n\} : \prod_{i=1}^n \ell_i \models H$, where Q_i stands for “there is” if $Q_i = \exists$ and for “for all” if $Q_i = \forall$.

Here, \models is the propositional consequence relation and \top the tautological truth.

Proof. Induction. ◀

¹ A path is *simple* if it does not visit a world twice.

► **Definition 3.2.** Let $\mathcal{M} = (W, R, V)$ be a Kripke model, π an R -path and $\psi = Q_1x_1 \dots Q_nx_nH$ a qbf. Say that π *implements* ψ if $Q_1\ell_1 \in \{x_1, \neg x_1\} \dots Q_n\ell_n \in \{x_n, \neg x_n\}$ there is a world w on π such that $V(w) \models \{\ell_1, \dots, \ell_n, H\}$.

► **Lemma 3.3.** *If a qbf $\psi = Q_1x_1 \dots Q_nx_nH$ is implemented by a path, then $\psi \equiv \top$.*

Proof. Assume \mathcal{M} and π as in 3.2. Then $Q_1\ell_1 \in \{x_1, \neg x_1\} \dots Q_n\ell_n \in \{x_n, \neg x_n\}$ there is a world w on π with $V(w) \models \{\ell_1, \dots, \ell_n, H\}$.

$\prod_{i=1}^n \ell_i$ implies either H or $\neg H$ as H contains no propositions other than x_1, \dots, x_n . But $\prod_{i=1}^n \ell_i \models \neg H$ would imply $V(w) \models \neg H \cdot H$, which contradicts V being a valuation. Hence it is $\prod_{i=1}^n \ell_i \models H$ and it follows $\psi \equiv \top$ by Lemma 3.1. ◀

► **Theorem 3.4.** $\text{SAT}(\mathcal{B}_2(\text{AF}))$ is \leq_m^{\log} -hard for **PSPACE**.

The problem QBF was proven \leq_m^{\log} -complete for **PSPACE** by Stockmeyer and Meyer [MS73]. The well-known reduction in literature from QBF to modal satisfiability for K or S4 [Lad77] does not work here as the operators AF and EG have “mixed” path and state quantifiers. As the constraints imposed by multiple F operators alone can always be fulfilled on paths of linear length, and satisfiability would therefore be efficiently verifiable, they have to somehow be embedded into G-preceded formulas for a meaningful reduction. But as G is only provided in its existentially quantified form, the whole work of the reduction from QBF has to happen on a single path (which is the path mentioned in 3.2). A consequence of this is that $\mathcal{B}_2(\text{AF})$ can enforce exponentially long paths.

Proof of Theorem 3.4. Let $\psi = Q_1x_1 \dots Q_nx_nH$ be a qbf. Formally, the reduction maps ψ to a formula $\varphi(\psi) \in \mathcal{B}_2(\text{AF})$ that is satisfiable if and only if ψ is true. The idea is to enforce a long path in the model which is successively subdivided into segments. The first half should uniformly render x_1 true, while on the other half $\neg x_1$ holds. Each of the segments is then again divided to account for the possible truth values of x_2 , and so on. With this approach a full binary assignment tree of x_1, \dots, x_n can be embedded into a single path in a Kripke structure.

We implement this by several propositions. The variables t_i and t'_i span a subsequence as a part of the model where x_i is enforced to be true. Conversely f_i and f'_i span a sequence of worlds where x_i is false. This is enforced by the formula γ_i . The formulas α_i^\forall and α_i^\exists are responsible for the mentioned subdivision of a path: In one case, both the “true” and “false” subsegments are forced to appear in this order. In the second case one can be chosen to adhere to the semantics of the quantifier Q_i . The formula β_i ensures that there is no unwanted “overlapping” of segments: If every b_i on the main path already implies $\text{EG}b_i$, then all the eventualities (AF-subformulas) in $\alpha_i^{Q_i}$ have to be fulfilled before b_i appears on it, as they ultimately imply $\text{AF}\neg b_i$.

Finally, the underscored variants $\underline{t'_i}, \underline{f_i}, \underline{f'_i}$ are propositions which function as placeholders to keep the temporal nesting depth low in this reduction.

$$\varphi(\psi) := s_1 \cdot \text{EG} \left[H \cdot \prod_{i=1}^n (\alpha_i^{Q_i} \cdot \beta_i \cdot \gamma_i) \right]$$

where

$$\begin{aligned}
\alpha_i^\forall &:= (s_i \rightarrow \text{AF}(t_i \cdot \neg s_i \cdot \neg b_i \cdot s_{i+1} \cdot \underline{t'_i})) \cdot \\
&\quad (\underline{t'_i} \rightarrow \text{AF}(t'_i \cdot \neg b_i \cdot b_{i+1} \cdot \underline{f_i})) \cdot \\
&\quad (\underline{f_i} \rightarrow \text{AF}(f_i \cdot \neg b_i \cdot s_{i+1} \cdot \underline{f'_i})) \cdot \\
&\quad (\underline{f'_i} \rightarrow \text{AF}(f'_i \cdot \neg b_i \cdot b_{i+1})), \\
\alpha_i^\exists &:= s_i \rightarrow \sum_{p \in \{t, f\}} \text{AF}(p_i \cdot \neg s_i \cdot \neg b_i \cdot s_{i+1}) \cdot \text{AF}(p'_i \cdot \neg b_i \cdot b_{i+1}), \\
\beta_i &:= (b_i \rightarrow \text{EG}b_i) \cdot (t'_i \rightarrow \text{EG}\neg t_i) \cdot (f_i \rightarrow \text{EG}\neg t'_i) \cdot (f'_i \rightarrow \text{EG}\neg f_i)
\end{aligned}$$

and

$$\gamma_i := (\text{AF}t'_i \rightarrow x_i) \cdot (\text{AF}f'_i \rightarrow \neg x_i).$$

For a model \mathcal{M} of $\varphi(\psi)$ the path satisfying the outermost EG operator is called *primary path* of \mathcal{M} . Consider the following abbreviations:

- $\pi[j..k]$ for the finite subpath $(\pi[j], \pi[j+1], \dots, \pi[k-1], \pi[k])$
- $\pi[j] \preceq \pi[k]$ if $j \leq k$ and $\pi[j] \prec \pi[k]$ if $j < k$
- $\pi' \leq \pi$ if $\pi' = \pi[j..k]$ for some $j, k, j \leq k$
- $\pi' < \pi$ if $\pi' = \pi[j..k]$ but there are w, w' on π with $w \prec \pi[j]$ and $\pi[k] \prec w'$.

Claim (a). Let \mathcal{M} be a model of $\varphi(\psi)$ and π its primary path. Then it holds for all $1 \leq i \leq n$: If there are j, k with $j < k$, $\pi[j] \models s_i$, $\pi[k] \models b_i$, then $\mathcal{Q}_i \ell_i \in \{x_i, \neg x_i\} : \exists \pi' \leq \pi[j..k] : \pi' \models \text{G}\ell_i$ and $\exists j', k'$ s.t. $j' < k'$, $\pi'[j'] \models s_{i+1}$ and $\pi'[k'] \models b_{i+1}$.

In other words: If π has s_i labeled in some world, then there is a subpath (or two subpaths, depending on \mathcal{Q}_i) induced between s_i and the next b_i . That subpaths have the property that on the one hand they “fix” the literal ℓ_i and on the other hand again have labeled s_{i+1} and b_{i+1} in this order.

Proof of claim. Assume that for $j < k$ it holds $\pi[j] \models s_i$ and $\pi[k] \models b_i$. First notice that $\pi[k] \models \text{EG}b_i$. Assume that $\mathcal{Q}_i = \forall$ (the case $\mathcal{Q}_i = \exists$ is proven similar). Then there are worlds $w_t, w_{t'}, w_f, w_{f'}$ on π with $\pi[j] \prec w_t \prec w_{t'} \prec w_f \prec w_{f'} \prec \pi[k]$ such that $w_t, w_{t'}, w_f, w_{f'}$ fulfill the eventualities imposed by the AFs in α_i and α_i^\forall . Then $w_p \models p_i$ for $p \in \{t, t', f, f'\}$, and $w_t, w_f \models s_{i+1}$, $w_{t'}, w_{f'} \models b_{i+1}$.

The AF formulas impose the eventualities to be fulfilled in different worlds, and exactly in this order. This is enforced due to α_i (in the \forall case) or β_i (in the \exists case): As $w_{t'} \models \text{EG}\neg t_i$ it must hold $w_t \prec w_{t'}$, and so on. That they have to be fulfilled before reaching the world $\pi[k]$ follows from $\pi[k] \models \text{EG}b_i$, i.e., they cannot be fulfilled once $\pi[k]$ is reached due to the duality of $\text{EG}b_i$ and $\text{AF}\neg b_i$.

To prove that w_t and $w_{t'}$ resp. w_f and $w_{f'}$ span the desired subpaths, it remains to show that x_i holds on every world between w_t and $w_{t'}$, and that $\neg x_i$ holds on every world between w_f and $w_{f'}$. But due to γ_i this is the case: Indeed for every world between (including) w_t and $w_{t'}$ it holds $\text{AF}t'_i$ and therefore x_i . Also for every world between (including) w_f and $w_{f'}$ it holds $\text{AF}f'_i$ and therefore $\neg x_i$. ■

Claim (b). If $\varphi(\psi)$ is satisfiable, then $\psi \equiv \top$.

Proof of claim. Due to Lemma 3.3 it suffices to find an implementing path π in a model of $\varphi(\psi)$, which is in this case the primary path. As $\pi \models \text{GH}$ we only have to prove that $\mathcal{Q}_1 \ell_1 \in \{x_1, \neg x_1\} \dots \mathcal{Q}_n \ell_n \in \{x_n, \neg x_n\}$ there is a world w on π s.t. $V(w) \models \{\ell_1, \dots, \ell_n\}$.

This is implied by

$$\begin{aligned}
Q_1 \ell_1 \in \{x_1, \neg x_1\} \quad \exists \pi^{(1)} \leq \pi & : \pi^{(1)} \models G\ell_1 : \\
Q_2 \ell_2 \in \{x_2, \neg x_2\} \quad \exists \pi^{(2)} \leq \pi^{(1)} & : \pi^{(2)} \models G\ell_2 : \\
& \dots \\
Q_n \ell_n \in \{x_n, \neg x_n\} \quad \exists \pi^{(n)} \leq \pi^{(n-1)} & : \pi^{(n)} \models G\ell_n \text{ and } \pi^{(n)} \text{ is non-empty,}
\end{aligned}$$

but since $\pi[0] \models s_1$ the fact can in turn be shown by n -fold application of Claim (a) (even if there is no terminating b_1). ■

Claim (c). $\varphi(\psi)|_{H/\top}$ is satisfiable, i.e., the formula obtained from $\varphi(\psi)$ by replacing H with \top .

Proof of claim. A model is constructed stepwise by n -fold path subdivision as follows. Write $\varphi|_i$ for the formula that is obtained from $\varphi(\psi)$ by ignoring not only H but also all $\alpha_i, \beta_i, \gamma_i$ subformulas with indices $> i$ (i.e. replacing them with \top). We show by induction that $\mathcal{M}_i \models \varphi|_i$, where \mathcal{M}_i is the model after the i -th construction step. It will consist of a primary path π which is recursively subdivided. The i -th subdivision shall be the modification of π that expands all pairs $(\pi[j], \pi[j+1])$ of worlds for which $\pi[j] \models s_i$ and $\pi[j+1] \models b_i$ in a way s. t. the subpath required by $\alpha_i^{Q_i}$ is inserted.

Start with a structure \mathcal{M}_0 only consisting of a primary path π of two worlds with $\pi[0] \models s_1$ and $\pi[1] \models b_1$, and $\pi[1]$ having a self-loop. If $n = 0$ then \mathcal{M}_0 already satisfies $\varphi(\psi)|_{H/\top}$. For the induction step assume that $\mathcal{M}_{i-1} \models \varphi|_{i-1}$. Let $(\pi[j], \pi[j+1])$ be a pair of worlds where s_i resp. b_i hold. Between them insert worlds w_p for $p = t, t', f, f'$ in this order. Set $L(w_t) = \{t_i, x_i, s_{i+1}, t'_i\}$, $L(w_{t'}) = \{t'_i, x_i, b_{i+1}, f_i\}$, $L(w_f) = \{f_i, s_{i+1}, f_i\}$ and finally $L(w_{f'}) = \{f'_i, b_{i+1}\}$. This fulfills necessary α formulas and the contained AFs. To have β_i and γ_i holding on this subpath without contradicting x_i literals it is required that $\text{AF}t'_i$ becomes false in the parts of the model where $\neg x_i$ should hold, and conversely $\text{AF}f'_i$ becomes false where x_i should hold. In other words, we require the following:

$$\begin{aligned}
w_t & \models \text{EG} \neg f'_i \\
w_{t'} & \models \text{EG} \neg f'_i \cdot \text{EG} \neg t_i \cdot \text{EG} b_{i+1} \\
w_f & \models \text{EG} \neg t'_i \\
w_{f'} & \models \text{EG} \neg t'_i \cdot \text{EG} \neg f_i \cdot \text{EG} b_{i+1}.
\end{aligned}$$

Therefore add a branch to $w_{t'}$ with a single world that has $\{f_i, f'_i, s_{i+1}, b_{i+1}\}$ labeled and a self-loop at the end. With this branch, the eventualities imposed by α_i resp. α_i^{\exists} in $w_{t'}$ are still fulfilled for any path from $w_{t'}$. Also add a branch to $w_{f'}$ with a single world that has a self-loop and only b_{i+1} labeled. Finally copy the literals $\ell_o \in \{x_o, \neg x_o\}$ for all $o < i$ from the surrounding $\pi[j]$ and $\pi[j+1]$ (they have to be the same).

The only remaining problem is again that the new branches can violate eventualities that are imposed on π *before* $\pi[j]$ but fulfilled *after* the former $\pi[j+1]$. We have to show that those eventualities can also be fulfilled on the two new branches while keeping their EG formulas intact. Fortunately, such eventuality can again only be of the form

$$\text{AF}(t'_o \cdot \neg b_o \cdot b_{o+1} \cdot \underline{f}_o)$$

or

$$\text{AF}(f'_o \cdot \neg b_o \cdot b_{o+1})$$

for some $o < i$. Both added branches allow the prolonging by additional worlds and the adding of the labels $\{t'_o, b_{o+1}, f'_o, f_o\}$ to these worlds. As $o < i$ this does not violate the EG formulas fulfilled by the branches. Thus $\mathcal{M}_i \models \varphi|_i$. ■

Claim (d). If $\psi \equiv \top$, then $\varphi(\psi)$ is satisfiable.

Proof of claim. A structure \mathcal{M} is constructed as in Claim (c) to satisfy $\varphi(\psi)|_{H/\top}$. To get a model for $\varphi(\psi)$, it should hold $\pi \models GH$ for the primary path π in the constructed structure \mathcal{M} . Notice that for $n = 0$ it is $H = \top$ and there is nothing to do.

To achieve this for $n > 0$, some parts of the structure have to be deleted, namely those worlds w on π with $V(w) \models \neg H$. Then it holds that the resulting structure is still a model of $\varphi(\psi)|_{H/\top}$ and thus of $\varphi(\psi)$. It may not be obvious that the α subformulas are still satisfied. But it holds that $Q_1 \ell_1 \in \{x_1, \neg x_1\}$ s. t. $Q_2 \ell_2 \in \{x_2, \neg x_2\} \dots Q_n \ell_n \in \{x_n, \neg x_n\} : \bigwedge_{i=1}^n \ell_i \models H$. Thus for $Q_i = \exists$ there is at least one subpath remaining between pairs of s_i and b_i , and for $Q_i = \forall$ both subpaths are retained, fulfilling the corresponding α subformulas. ■

The claims (b) and (d) show that $\psi \equiv \top$ if and only if $\varphi(\psi)$ is satisfiable. Also $\varphi(\psi)$ is constructible in logarithmic space and has temporal depth ≤ 2 . Therefore it follows

$$\text{QBF} \leq_{\text{m}}^{\log} \text{SAT}(\mathcal{B}_2(\text{AF})).$$

◀

► **Corollary 3.5.** $\mathcal{B}_k(\text{AF})$ and $\mathcal{B}(\text{AF})$ have optimal model size and depth $2^{\Theta(n)}$ for all $k \geq 2$.

It may be surprising at first sight that AF can enforce a single exponentially long path while F and G cannot do this for LTL. The reason for this is twofold: On the one hand F operators follow a certain kind of “order invariance”: At a certain point a path fulfills all G formulas that are ever labeled on it; from this point the order of fulfillment of F does not matter. On the other hand, all G formulas occurring on a path obviously have a common scope by not being allowed to branch and therefore have to be consistent. Paths witnessing an EG subformula may “branch off” arbitrarily. Both properties are used by Sistla and Clarke to show the small model property [SC85], while conversely the absence of both properties is crucial for the proof presented here.

3.2 The AG fragment

Not much new is to show for the computational complexity of this fragment. In terms of satisfiability, it is equivalent to modal logic on S4D-frames, i.e., transitive, reflexive and serial. We will improve the results known for this logic in the sense that the lower bound already holds for temporal depth two.

► **Theorem 3.6.** $\text{SAT}(\mathcal{B}_2(\text{AG}))$ is \leq_{m}^{\log} -hard for PSPACE.

Proof. We again map a qbf ψ to a formula $\varphi(\psi)$ that is satisfiable if and only if the qbf ψ is true. While the idea is roughly the same as the previous theorem—force a Kripke structure to carry up to 2^n different propositional assignments—the implementation fundamentally differs due to the different semantics of AF and AG. When using the first operator we must use a single exponentially long path, and with the second we have an exponentially branching tree with linear depth. We will later see a matching upper bound for the optimal model depth.

Let $\psi = Q_1 x_1 \dots Q_n x_n H$ again be a qbf. Then the formula $\varphi(\psi)$ is defined as follows:

$$\begin{aligned} \varphi(\psi) &:= \underline{x}_0 \cdot \text{AG} \left(H \cdot \prod_{i=1}^n \alpha_i \right) \\ \alpha_i &:= \left[(\underline{x}_{i-1} + \underline{x'_{i-1}}) \rightarrow (\text{EF} \underline{x}_i \circ_i \text{EF} \underline{x'_i}) \right] \cdot \left[\underline{x}_i \rightarrow \text{AG} \underline{x}_i \right] \cdot \left[\underline{x'_i} \rightarrow \text{AG} \neg \underline{x}_i \right] \end{aligned}$$

where

$$\circ_i := \begin{cases} \cdot & \text{if } Q_i = \forall \\ + & \text{if } Q_i = \exists \end{cases}$$

and the $\underline{x}_i, \underline{x'_i}$ are fresh propositional variables.

Claim. If $\varphi(\psi)$ has a model $\mathcal{M} = (W, R, V)$, then ψ is true.

Proof of claim. Let $w^{(0)}$ be the root of \mathcal{M} . Define $R^*(w) := \{ w' \mid w R^* w' \}$, i.e., as the set of all worlds reachable from w via an R -path.

The following facts can easily be verified by the above formulas. For all $1 \leq i \leq n$ and every world $w \in R^*(w^{(0)})$ it holds:

- if $\underline{x}_i \in V(w)$, then $\underline{x}_i \in V(w')$ for all worlds $w' \in R^*(w)$,
- if $\underline{x'_i} \in V(w)$, then $\underline{x}_i \notin V(w')$ for all worlds $w' \in R^*(w)$,
- if $Q_i = \forall$ and either \underline{x}_i or $\underline{x'_i}$ is in $V(w)$, then there are $w', w'' \in R^*(w)$ with $\underline{x_{i+1}} \in V(w')$ and $\underline{x'_{i+1}} \in V(w'')$
- if $Q_i = \exists$ and either \underline{x}_i or $\underline{x'_i}$ is in $V(w)$, then there is some $w' \in R^*(w)$ with either $\underline{x_{i+1}} \in V(w')$ or $\underline{x'_{i+1}} \in V(w')$

It holds $w^{(0)} \models \underline{x}_0$. Then from applying the above items n times we can derive:

$$\begin{aligned} Q_1 \ell_1 &\in \{x_1, \neg x_1\} \quad \exists w^{(1)} \in R^*(w^{(0)}) \quad \text{s.t. } w^{(1)} \models \ell_1 \text{ and} \\ Q_2 \ell_2 &\in \{x_2, \neg x_2\} \quad \exists w^{(2)} \in R^*(w^{(1)}) \quad \text{s.t. } w^{(2)} \models \ell_1 \cdot \ell_2 \text{ and} \\ &\dots \\ Q_n \ell_n &\in \{x_n, \neg x_n\} \quad \exists w^{(n)} \in R^*(w^{(n-1)}) \quad \text{s.t. } w^{(n)} \models \prod_{i=1}^n \ell_i. \end{aligned}$$

This implies: $Q_1 \ell_1 \in \{x_1, \neg x_1\} \dots Q_n \ell_n \in \{x_n, \neg x_n\}$ there is a world $w \in R^*(w^{(0)})$ such that $w \models \{\ell_1, \dots, \ell_n, H\}$. Then it cannot be the case that $\prod_{i=1}^n \ell_i \models \neg H$.

Instead $Q_1 \ell_1 \in \{x_1, \neg x_1\} \dots Q_n \ell_n \in \{x_n, \neg x_n\} : \prod_{i=1}^n \ell_i \models H$ holds, and the claim follows from Lemma 3.1. ■

Claim. If ψ is true, then $\varphi(\psi)$ is satisfiable.

Proof of claim. First we construct a binary tree which satisfies $\varphi(\psi)|_{H/\top}$, the formula obtained by replacing H with \top in $\varphi(\psi)$.

For this begin with a root world $w^{(0)}$ which has \underline{x}_0 labeled. Then for $i = 1, \dots, n+1$, there are two successors w, w' appended to each leaf of the previous step, where $w \models \underline{x}_i$ and $w' \models \underline{x'_i}$. Also for $j \leq i$ label x_j in any added world w if it is reachable from another world where \underline{x}_j holds. As occurrences of \underline{x}_j and $\underline{x'_j}$ always span distinct subtrees, this does not

introduce contradictions. After adding self-loops to the final leaves the resulting structure therefore models $\varphi(\psi)|_{H/\top}$.

To get a model for $\varphi(\psi)$, it suffices to delete the worlds w from \mathcal{M} with $V(w) \models \neg H$. This is analog to the last part of the proof of Theorem 3.4. The only subformulas that could be affected by this are the EF subformulas, but they stay fulfilled due to the construction. ■

As the given formula is constructible in logarithmic space, has temporal depth ≤ 2 and also is satisfiable if and only if ψ is true, it follows $\text{QBF} \leq_{\text{m}}^{\log} \text{SAT}(\mathcal{B}_2(\text{AG}))$. ◀

► **Theorem 3.7.** $\text{SAT}(\mathcal{B}(\text{AG})) \in \text{PSPACE}$.

Proof. As $\text{SAT}(\mathcal{B}(\text{AG}))$ is equivalent to S4D-satisfiability of modal logic, i.e., on transitive, serial, reflexive Kripke frames, the S4-satisfiability algorithm given by Ladner [Lad77] provides the desired result with little modifications to ensure seriality. ◀

The next result will be an upper bound for model depth. For this we introduce the notion of *quasi-models*. The crucial difference to a model is that we do not need to talk about *truth* of a subformula, but rather only whether a subformula or its negation is *necessitated* in a specific world at all. This approach is well-known in literature for establishing upper bounds for model size, often together with filtration techniques. Related notions are *Hintikka structures*, *pseudo-models* or *tableaux*.

► **Definition 3.8 (Closure).** Let C be a finite set of Boolean functions and $T \subseteq \text{TL}$. Let $\varphi \in \mathcal{B}(C, T)$. Then define $\sim\psi := \xi$ if $\psi = \neg\xi$ for some ξ , and $\sim\psi := \neg\psi$ otherwise. Further define $\bar{A} := E$, $\bar{E} := A$, $\bar{F} := G$, $\bar{G} := F$, $\bar{U} := R$, $\bar{R} := U$ and $\bar{X} := X$.

The *closure* $cl(\varphi)$ of φ is the smallest set for which holds:

- $\varphi \in cl(\varphi)$.
- if $QO \in \text{TL}$, $QO\psi \in cl(\varphi)$ (i.e., O is unary), then $\bar{Q}\bar{O}\sim\psi, \psi \in cl(\varphi)$,
- if $QO \in \text{TL}$, $Q[\psi O\xi] \in cl(\varphi)$ (i.e., O is binary), then $\bar{Q}[\sim\psi\bar{O}\sim\xi], \psi, \xi \in cl(\varphi)$,
- if $f(\psi_1, \dots, \psi_n) \in cl(\varphi)$, $f \in C$, then $\psi_1, \dots, \psi_n \in cl(\varphi)$,
- $\psi \in cl(\varphi)$ iff $\sim\psi \in cl(\varphi)$.

For a set Γ of formulas, define $cl(\Gamma) := \bigcup_{\gamma \in \Gamma} cl(\gamma)$.

The closure cl is related to the *Ladner-Fischer closure* defined for PDL [FL79]. Similar terms are *Hintikka set* or *downward saturated set*.

Note that \neg is used independently of whether there is $\neg \in C$, hence $cl(\varphi)$ is not necessarily a subset of $\mathcal{B}(C, T)$.

► **Definition 3.9 (Quasi-models).** Let $\varphi \in \mathcal{B}(C, \text{TL})$. A *quasi-model* of φ is then a tuple $\mathcal{Q} = (W, R, L)$ where (W, R) is a Kripke frame and $L: W \rightarrow \mathfrak{P}(cl(\varphi))$ is an *extended labeling function* with the following *quasi-label conditions*:

1. if $L(w)$ contains $f(\psi_1, \dots, \psi_n)$ resp. $\sim f(\psi_1, \dots, \psi_n)$ for some n -ary $f \in C$, then there is a Boolean assignment θ s. t. $\theta \models f$ resp. $\theta \not\models f$ and f.a. $i: \theta(i) = 1 \rightarrow \psi_i \in L(w)$ and $\theta(i) = 0 \rightarrow \sim\psi_i \in L(w)$,
2. if $\psi, \neg\xi \in L(w)$ then $\psi \neq \xi$
3. if $\sim QO\psi$ ($\sim Q[\psi O\xi]$) $\in L(w)$ for $QO \in \text{TL}$, then $\bar{Q}\bar{O}\sim\psi$ ($\bar{Q}[\sim\psi\bar{O}\sim\xi]$) $\in L(w)$,
4. if $E\psi$ ($A\psi$) $\in L(w)$, then for some (all) paths $\pi \in \Pi(w)$:
 - if $\psi = X\beta$, then $\beta \in L(\pi[1])$
 - if $\psi = F\beta$ ($G\beta$), then $\beta \in L(\pi[i])$ for some (all) $i \geq 0$,
 - if $\psi = \beta U\xi$ ($\beta R\xi$), then for some (all) $i \geq 0$ it is $\xi \in L(\pi[i])$ and (or) $\beta \in L(\pi[j])$ for all (some) $j < i$,
5. $\varphi \in L(w)$ for some $w \in W$.

$L(w)$ is the *quasi-label* of a world w . The numbers 1. to 3. are the *local* quasi-label conditions.

► **Lemma 3.10.** $\varphi \in \mathcal{B}(C, \text{TL})$ has a model of size s and depth d if and only if it has a serial quasi-model of size s and depth d . Furthermore, $\varphi \in \mathcal{B}(C, \text{TL})$ is satisfiable iff it has an infinite serial tree quasi-model.

Proof. From a model \mathcal{M} of φ we can define a quasi-model by choosing $L(w) := \{ \psi \mid \psi \in cl(\varphi) \text{ and } w \models \psi \}$. Conversely from a quasi-model all labeled formulas can be dropped except atomic propositions to obtain a model.

The equivalence of infinite tree models was shown by Allen Emerson as a by-product of the finite model property [AE90, Thm. 6.14]. ◀

► **Theorem 3.11.** $\mathcal{B}_k(\text{AG})$ and $\mathcal{B}(\text{AG})$ have optimal model size $2^{\Theta(n)}$ and depth $\Theta(n)$ for all $k \geq 2$.

Proof. The lower bounds both follow from the reduction from QBF which is part of the hardness proof, see Theorem 3.6. The upper bound for the size is inherited from full CTL (Theorem 2.9).

For the upper bound for depth consider some satisfiable $\varphi \in \mathcal{B}(\text{AG})$.

Let $\mathcal{T} = (W, R, L)$ then be an infinite tree quasi-model of φ . For a world w write \mathcal{F} for the set of its labeled EF-prefixed formulas and similar \mathcal{G} for its labeled AG-prefixed formulas. We can assume the following about \mathcal{T} : If $\text{AG}\psi \in L(w)$ for some world w , then not only ψ is labeled in all reachable worlds, but also $\text{AG}\psi$. This is still a valid quasi-model. Conversely, if $\text{EF}\psi \in L(w)$ for some world w , then either $\psi \in L(v)$ or $\text{EF}\psi \in L(v)$ for some R -successor v of w . Write $R_{\mathcal{F}} : \mathcal{F}(w) \rightarrow W$ for the map that assigns the corresponding R -successors. We can assume that $R_{\mathcal{F}}$ is total and injective, in other words, for every EF-prefixed labeled formula a distinct successor is selected which the witnessing path should visit immediately after w .

Define a new quasi-model $\mathcal{T}' = (W', R', L)$ where W', R' are some minimal sets s. t.

- W' contains the root of \mathcal{T} , and
- for all $w \in W'$ and all $\text{EF}\psi \in \mathcal{F}(w)$ it holds $u \in W'$ and $wR'u$, where u is a world with maximal $\mathcal{G}(u)$ under all those worlds u' with $\psi \in L(u')$ and $(R_{\mathcal{F}}(\text{EF}\psi))R^*u'$, in other words, from those worlds that are reachable from $R_{\mathcal{F}}(\text{EF}\psi)$ and also fulfill $\text{EF}\psi$ (such a world must exist).

Here, R^* is the reflexive transitive closure of R .

The construction corresponds to “greedily” choosing a substructure \mathcal{T}' contained in \mathcal{T} : \mathcal{T}' is defined level-by-level where any EF labeled in a world is always fulfilled in a distinct direct successor. Note that $\mathcal{G}(w) \subseteq \mathcal{G}(u)$ if $wR'u$, so the AGs stay fulfilled. Hence \mathcal{T}' is a quasi-model of φ .

Now consider an arbitrary path $\pi = (u_0, u_1, \dots)$ through \mathcal{T}' . For every non-root world u_i there is some $\text{EF}\psi = R_{\mathcal{F}}^{-1}(u_i)$. $R_{\mathcal{F}}^{-1}$ is the inverse of $R_{\mathcal{F}}$ and maps a world u_i to the corresponding $\text{EF}\psi$ formula in the predecessor, i.e., the “justification” why u_i exists. It holds that $\psi \in L(u_i)$.

Assume $R_{\mathcal{F}}^{-1}(u_i) = R_{\mathcal{F}}^{-1}(u_j) = \text{EF}\psi$ for some $i < j$. Then $\mathcal{G}(u_i) = \mathcal{G}(u_j)$. The only other possibility would be $\mathcal{G}(u_i) \subsetneq \mathcal{G}(u_j)$, but this is prevented by the choice of u in the construction of \mathcal{T}' .

Transform \mathcal{T}' to a finite model \mathcal{M} as follows: While there is a *long* path π , *furl* that path. A *long* path is one that visits more distinct non-root worlds than φ has EF operators. To *furl*

π choose the minimal j s. t. $R_{\mathcal{F}}^{-1}(\pi[j]) = R_{\mathcal{F}}^{-1}(\pi[i])$ for some $i < j$. Such an j must exist if π is long. The world $\pi[j]$ can simply be replaced by a back edge from $\pi[j-1]$ to $\pi[i]$ without violating any quasi-label condition. No AG condition is violated, as $\mathcal{G}(\pi[i]) = \mathcal{G}(\pi[j])$, and no EF condition is violated, as every labeled EF is always fulfilled by a distinct successor resp. back edge. It holds that by construction \mathcal{T}' has finite branching, i.e., every world has finitely many successors. Thus this procedure must terminate, and as \mathcal{M} now has no long paths anymore, all its simple paths have length at most $|\varphi|$. ◀

3.3 The AX fragment

In the context of temporal logics, not much is to say about the AX fragment except referring the reader to literature about standard modal logic. The next theorems reproduce standard results.

► **Theorem 3.12.** $\mathcal{B}(\text{AX})$ has optimal model size $2^{\Omega(\sqrt{n})} \cap 2^{\mathcal{O}(n)}$ and depth $\Theta(n)$.
For each $k \geq 0$, $\mathcal{B}_k(\text{AX})$ has optimal model size $\Theta(n^{\Theta(k)})$ and depth k .

Proof. Let

$$\psi_i^m := \prod_{j=0}^{m-1} \text{EX} \vec{c}_i(j) \cdot \prod_{s=1}^{i-1} \prod_{t=0}^{\lceil \log m \rceil} (p_{s,t} \rightarrow \text{AX} p_{s,t}) \cdot (\neg p_{s,t} \rightarrow \text{AX} \neg p_{s,t})$$

where $\vec{c}_i(j)$ is a conjunction of $\lceil \log m \rceil$ Boolean propositions $p_{i,1}, \dots, p_{i,\lceil \log m \rceil}$ representing j as a binary vector.

The formula $\psi_1^m \wedge \text{AX}(\psi_2^m \wedge \text{AX}(\dots (\text{AX} \varphi_k^m)))$ has length $\mathcal{O}(k^2 \cdot m \log m)$, temporal depth k and no model smaller than m^k . For fixed m and unbounded k we see that there are satisfiable formulas of length $\mathcal{O}(k^2)$ with minimal model size of $2^{\Omega(k)}$. The latter case is in fact a well-known example for a modal formula enforcing a large model [Mar07, Prop. 9]. For fixed k and unbounded m the given example results in satisfiable formulas of length $\mathcal{O}(m \log m)$ with minimal model size of $m^{\Theta(k)} \subseteq (m \log m)^{\Theta(k)}$.

The temporal depth as an upper bound for the model depth can easily be shown by induction. The upper bound for size for fixed k then follows from the fact that every world requires at most $|\varphi|$ successors and $\sum_{i=0}^k |\varphi|^i \in \mathcal{O}(|\varphi|^k)$. For unbounded k see Theorem 2.9. ◀

► **Theorem 3.13.** $\text{SAT}(\mathcal{B}_k(\text{AX}))$ is NP-complete under \leq_m^{\log} -reduction for each $k \in \mathbb{N}$.

Proof. The upper bound follows from the previous theorem: Guess a satisfying model of polynomial size and verify it in polynomial time as CTL model checking is in **P** [CAES86]. The lower bound holds as \mathcal{B}_0 is nothing else than propositional logic for which the satisfiability problem is already NP-complete under \leq_m^{\log} [Coo71]. ◀

► **Theorem 3.14.** $\text{SAT}(\mathcal{B}(\text{AX}))$ is PSPACE-complete under \leq_m^{\log} -reduction.

Proof. $\text{SAT}(\mathcal{B}(\text{AX}))$ is equivalent to D-satisfiability of modal logic, i.e., on serial frames, thus the problem is in **PSPACE**. For the **PSPACE**-hardness, the reduction from QBF done by Ladner [Lad77] can easily be modified to produce only serial frames. ◀

3.4 The AF AX fragment

The next part establishes the matching upper bounds for the fragment with both AX and AF. It requires some technical work; we show **PSPACE** membership by constructing a canonical model, the *balloon model*. This canonical model has a special form which allows to non-deterministically construct it and verify it on-the-fly, namely it is “pseudo-acyclic”: It almost resembles a tree, except that its branches are closed into cycles. This strong restriction to possible back-edges allows to guess such a model using only polynomial space.

► **Definition 3.15.** A *balloon path* of length n is a structure (W, R) where $|W| \leq n$, every world has exactly one R -successor and one world (the root) has no R -predecessor. Therefore it always consists of a single path which has a non-empty *prefix* followed by a non-empty *cycle*. If the underlying structure is clear from the context, the path itself will also be called *balloon path*.

A *balloon structure* \mathcal{M} of level m and length n is defined as follows:

- if $m = 0$ then \mathcal{M} is a balloon path of length n .
- if $m > 0$ then \mathcal{M} is constructed by taking a balloon path of length n and appending to each non-root world u a finite number of balloon structures of level at most $m - 1$ and length n . *Appending* here means identifying each of their roots with u s.t. they have no other worlds in common with each other or with \mathcal{M} .

Such a structure \mathcal{M} has some useful properties, e.g., it holds that every path must visit at most one balloon of level $m, m - 1, \dots, k$ for some $k \geq 1$, and then stay forever in that one with level k .

If (W, R) is a balloon structure and (W, R, L) is a quasi-model of a formula φ , then $\mathcal{M} = (W, R, L)$ is a *balloon quasi-model* of φ . Say that \mathcal{M} is *branching-normalized* if either it has level 0 or for all worlds u there is a bijection between E-prefixed formulas γ labeled in u and paths emanating from u into a balloon of shallower level to fulfill γ .

► **Lemma 3.16** (Balloon lemma). *Let T be definable by $\{AX, AF\}$ under BF. Then $\varphi \in \mathcal{B}(T)$ is satisfiable if and only if it has a normalized balloon quasi-model of level $\mathcal{O}(|\varphi|)$ and balloon length $2^{\mathcal{O}(|\varphi|)}$.*

Proof. We use the following convention for quasi-models: Label any $AF\alpha$ in w if a predecessor w' of w has labeled $AF\alpha$, but neither w nor w' have α labeled. This way we can “track” the unfulfilled eventualities while retaining legal quasi-labels.

Let \mathcal{M} be an arbitrary quasi-model of φ . Let \mathcal{M} be a quasi-model of minimal size, hence $|\mathcal{M}| \in 2^{\mathcal{O}(|\varphi|)}$. We construct a branching-normalized balloon model \mathcal{T} by extracting paths from \mathcal{M} and inserting copies of them into \mathcal{T} .

A quasi-label is *minimal* if further removing of labeled formulas would violate a quasi-label condition (either locally or in a previous state), or would violate the convention mentioned above.

A path is *ultimately periodic* if it has the form $(w_0, \dots, w_i, w_{i+1}, \dots, w_{i+k}, w_i, w_{i+1}, \dots)$, i.e., it consists of a finite prefix followed by an infinite repetition of a finite, non-empty cycle. For such an infinite path define its *length* as the sum of the lengths of its prefix and its cycle.

Claim (a). If $E\gamma \in L(w)$ for some world w in \mathcal{M} , then there is a $\pi \in \Pi(w)$ that witnesses $E\gamma$ and is ultimately periodic with length at most $|\mathcal{M}| + 1$.

Proof of claim. First observe that any path π through \mathcal{M} must visit at least one world u of \mathcal{M} at least twice. Let $\pi \in \prod(w)$ be the path through \mathcal{M} that witnesses the formula $E\gamma$, and choose u as the first world occurring a second time on π . Now it holds that every eventuality imposed until the first occurrence of u must be fulfilled before the second occurrence of u . Otherwise there would be a path in \mathcal{M} on which some eventualities are never fulfilled: just go from w to u and repeat the cycle from u to u infinitely often. But as \mathcal{M} is a quasi-model, we can choose exactly this path as it witnesses $E\gamma$ and is ultimately periodic and of length at most $|\mathcal{M}| + 1$. ■

Now to the construction of \mathcal{T} . Select any world r of \mathcal{M} with $\varphi \in L(r)$ as the root of \mathcal{T} . Assume it contains at least one E-formula. Then, for every formula $E\gamma \in L(w)$ in some world w in \mathcal{T} select a path π from \mathcal{M} which witnesses γ and is ultimately periodic with length $2^{\mathcal{O}(|\varphi|)}$. Append this path to w . If the appended path happens to have an empty prefix, i.e., $\pi = (u, v_1, \dots, v_m, u, v_1, \dots, v_m, \dots)$, then insert a prefix (u', v'_1, \dots, v'_m) of copies of each world in the cycle. Then the resulting path is a balloon path and equivalent in terms of its labels. After every insertion of a path, minimize all quasi-labels in \mathcal{T} .

It remains to show that the resulting balloon quasi-model has at most level $\mathcal{O}(|\varphi|)$.

For the rest of the proof we assume that subformulas can occur multiple times in φ only if they are atomic propositions. This kind of syntactic uniqueness eases the technical argumentation, but does not restrict its validity (for instance one could just replace symbols O from T or C by variants O', O'', \dots with the same semantical meaning). Say that a formula $\psi \in \Gamma$ is *maximal* in Γ if there is no formula $\psi' \in \Gamma$, $\psi' \neq \psi$, $\psi \in cl(\psi')$.

Let u be an arbitrary world on a balloon π in \mathcal{T} s.t. π has root $w \neq u$ and was added for fulfilling $E\gamma \in L(w)$. Then the following two claims hold.

Claim (b). $cl(L(u)) \subseteq cl(L(w)) \subseteq cl(\varphi)$.

Proof of claim. Let $\psi \in cl(L(u))$. Then there is exactly one maximal $\psi' \in L(u)$ with $\psi \in cl(\psi')$. There must be some $\beta \in L(w)$ which contains ψ' or $\sim\psi'$, as \mathcal{M} has only minimal quasi-labels and a maximal formula cannot be locally enforced in a minimal quasi-label, but must be justified by some formula in a previous state. This formula must occur in $cl(L(w))$. Hence $\psi \in cl(\psi') \subseteq cl(\beta) \subseteq cl(L(w))$. That $cl(L(w)) \subseteq cl(\varphi)$ follows from the definition of a quasi-model. ■

Claim (c). $cl(L(u)) \subsetneq cl(L(w))$.

Proof of claim. Assume the contrary; then $cl(L(u)) = cl(L(w))$ due to the previous claim. It is $E\gamma \in L(w) \subseteq cl(L(w)) = cl(L(u))$, thus there must be a maximal formula $\gamma' \in L(u)$ with $E\gamma \in cl(\gamma')$, but a maximal formula again cannot be locally enforced. Instead it is justified by some maximal $A\alpha$ in $L(w)$ which contains γ' . Its outermost symbol must be in fact be **A**: The only E-preceded formula in $L(w)$ which could affect u would be $E\gamma$. But γ cannot contain γ' as we assume syntactical uniqueness of composite subformulas.

Distinguish three cases regarding $A\alpha$: Either α starts with **X**, or α starts with **F** and is already fulfilled in w ; or it is not. The first and third case are immediately ruled out: Due to syntactical uniqueness there would be no necessity to have $E\gamma \in L(w)$ and hence π would not even exist in a minimal model.² Therefore α starts with **F** and $A\alpha$ is immediately fulfilled in w .

² Note that exactly this part of the proof fails when **AG**, **AU** or **AR** is available, as they *do* necessitate labeled subformulas with or without fulfillment.

But as $cl(L(w)) = cl(L(u))$ it is still $A\alpha \in cl(L(u))$, despite $A\alpha$ being fulfilled in w . Hence there must again be some maximal $\alpha' \in L(u)$ with $A\alpha \in cl(\alpha')$ and some strictly larger $A\alpha'' \in L(w)$ with α'' containing α' . But this contradicts the maximality of $A\alpha$ under those formulas in $L(w)$ containing γ' . ■

As $cl(L(r)) = cl(\varphi)$ and $|cl(\varphi)| \in \mathcal{O}(|\varphi|)$, it follows that \mathcal{T} is a balloon quasi-model of level $\mathcal{O}(|\varphi|)$. That \mathcal{T} is branching-normalized and has balloon length $2^{\mathcal{O}(|\varphi|)}$ follows from the construction. ◀

► **Theorem 3.17.** *Let T be definable by $\{AX, AF\}$. Then $SAT(\mathcal{B}(T)) \in \mathbf{PSPACE}$.*

Algorithm 1: NPSpace algorithm for $SAT(\mathcal{B}(C, \{AF, EG, AX, EX\}))$

Input : $\varphi \in \mathcal{B}(C, T)$ where $T \subseteq \{AF, EG, AX, EX\}$

Output: Is φ satisfiable?

```

1 /*  $\mathcal{G}$ : EG formula to satisfy */
2 /*  $\mathcal{F}_{\text{root}}$ : unfulfilled eventualities at the root of the balloon */
3 /*  $\mathcal{X}_{\text{root}}$ : unfulfilled X formulas at the root of the balloon */
4 /*  $d$ : remaining depth counter */
5 Procedure guesspath( $\mathcal{G}, \mathcal{F}_{\text{root}}, \mathcal{X}_{\text{root}}, d$ )
6   if  $d = 0$  then return false
7   guess  $t \in \{1, \dots, 2^{m \cdot |\varphi|}\}$  /* world where the cycle is closed */
8    $\mathcal{X} := \mathcal{X}_{\text{root}}; \mathcal{F} := \mathcal{F}_{\text{root}}; \mathcal{F}^* := \emptyset; L^* := \emptyset$ 
9   for  $i := 0$  to  $2^{m \cdot |\varphi|}$  do
10     guess a quasi-label  $L$ 
11     if  $L$  violates a local quasi-label condition then return false
12     if  $\mathcal{X} \not\subseteq L$  then return false
13     if  $\mathcal{G} \not\subseteq L$  then return false
14      $\mathcal{X} := \{\psi \mid AX\psi \in L\}$ 
15     foreach  $AF\psi \in L$  do
16       add  $AF\psi$  to  $\mathcal{F}$ 
17     foreach  $\psi \in L$  do
18       remove  $AF\psi$  from  $\mathcal{F}$  and  $\mathcal{F}^*$ 
19     if  $i = t$  then
20        $L^* := L$  /* must be equal when closing the cycle */
21        $\mathcal{F}^* := \mathcal{F}$  /* must be fulfilled before closing the cycle */
22     foreach  $EG\gamma \in L$  do
23       if not guesspath( $\{\gamma\}, \mathcal{F}, \mathcal{X}, d - 1$ ) then return false
24     foreach  $EX\xi \in L$  do
25       if not guesspath( $\emptyset, \mathcal{F}, \mathcal{X} \cup \{\xi\}, d - 1$ ) then return false
26     if  $i \geq t$  and  $\mathcal{F}^* = \emptyset$  and  $L = L^*$  then return true
27   return false /* could not fulfill all eventualities */
28 return guesspath( $\emptyset, \emptyset, \{\varphi\}, m \cdot |\varphi|$ )

```

Proof. As $\mathbf{NPSpace} = \mathbf{PSPACE}$ we consider the non-deterministic Algorithm 1 that runs in polynomial space. The algorithm uses the previous lemma and verifies the existence

of a balloon quasi-model by traversing its balloon paths on-the-fly and recursively descending into deeper balloon levels as necessary.

There is an $m \in \mathbb{N}$ s. t. φ is satisfiable iff it has balloon quasi-model with balloon length $2^{m \cdot |\varphi|}$ and level $m \cdot |\varphi|$. This allows the algorithm to non-deterministically construct the balloon model in a top-down depth-first search manner. A single balloon path is constructed by guessing the back edge (which is represented as a pointer t of linear length) and consecutively guessing the quasi-labels on this path. This also works in polynomial space as visited labels can be “forgotten” immediately. Finally the recursion depth is only linear as the level of recursion corresponds to the level of the balloon path, hence the overall space requirement is quadratic. \blacktriangleleft

3.5 Hard fragments

► **Theorem 3.18.** $\text{SAT}(\mathcal{B}_2(T))$ is **EXP**-hard under \leq_m^{\log} -reduction if $\text{AU} \in T$, $\text{AR} \in T$, $\{\text{AG}, \text{AX}\} \subseteq T$ or $\{\text{AG}, \text{AF}\} \subseteq T$.

Proof. To show this lower bound, a known method in literature is a generic reduction from **APSPACE** [AEH85, MMTV09] as **APSPACE** = **EXP** [CKS81].

APSPACE (alternating polynomial space) is the class of sets decided by *alternating polynomial space-bounded single-tape Turing machines (pspace-ATMs)*.

Define an *alternating Turing machine* as a tuple $(Q_\exists, Q_\forall, \Sigma, \Gamma, \delta, q_0, \square, q_{\text{acc}}, q_{\text{rej}})$, where Q_\exists, Q_\forall are disjoint sets of *existentially branching* and *universally branching* states, $Q := Q_\exists \cup Q_\forall$ is the set of all states, $q_{\text{acc}}, q_{\text{rej}} \in Q$ are the *accepting* resp. *rejecting* state, $q_0 \in Q$ is the initial state, $\Sigma \subseteq \Gamma$ and Γ are the input and tape alphabet, $\square \in \Gamma \setminus \Sigma$ is the *blank symbol* and $\delta: Q \times \Gamma \rightarrow \mathfrak{P}(Q \times \Gamma \times X)$ is the *transition function*, where $X = \{-1, 0, 1\}$ and $\delta(q, a)$ is a finite set f.a. $q \in Q, a \in \Gamma$.

A *configuration* is a tuple (q, i, t) where $q \in Q$ is the current state, $i \in \mathbb{N}$ is the current *head position* and $t \in \Gamma^*$ the current *tape content*. Write $\delta(q, i, t)$ for the set of all configurations resulting from applying a transition of $\delta(q, t_i)$. Then a configuration *accepts* if $q = q_{\text{acc}}$; or if $\delta(q, i, t)$ contains at least one configuration that accepts and $q \in Q_\exists$; or if it contains only accepting configurations and $q \in Q_\forall$. Also $q \neq q_{\text{rej}}$ must hold. An ATM M accepts an input $x \in \Sigma^*$ if the initial configuration $(q_0, 1, x)$ accepts. An ATM M runs in *polynomial space* if there is a polynomial g s. t. on each input x the head position i is always in $\{1, \dots, g(|x|)\}$ (we can assume that M does not leave the input to the left).

Let $A \in \mathbf{APSPACE}$, $A \subseteq \Sigma^*$ be a set which we will reduce to $\text{SAT}(\mathcal{B}_2)$. Then A is decided by a pspace-bounded ATM M . W.l.o.g. M is chosen s. t. $\delta(q, a)$ is always non-empty and that on all inputs every computation path eventually assumes the state q_{acc} or q_{rej} . That such an M can be chosen is proven similar to [CKS81, Thm. 2.6].

Case 1: AG, AX

The following CTL formula $\varphi \in \mathcal{B}_2(\text{AG}, \text{AX})$ is satisfiable if and only if the given pspace-bounded ATM M accepts on input x . It is constructible in space logarithmic in $|x|$. Let $I := \{1, \dots, g(|x|)\}$.

$$\begin{aligned} \varphi &:= \varphi_{\text{init}} \cdot \text{AG} \varphi_{\text{conf}} \cdot \text{AG} \varphi_\delta \cdot \text{AG} \varphi'_\delta \\ \varphi_{\text{init}} &:= s_{q_0} \cdot p_1 \cdot \prod_{1 \leq i \leq |x|} t_{i, x_i} \cdot \prod_{\substack{i \in I \\ i > |x|}} t_{i, \square} \end{aligned}$$

$$\begin{aligned}
\varphi_{\text{conf}} &:= \sum_{q \in Q} \left(s_q \cdot \prod_{q' \in Q \setminus \{q\}} \neg s_{q'} \right) \cdot \sum_{i \in I} \left(p_i \cdot \prod_{j \in I \setminus \{i\}} \neg p_j \right) \cdot \prod_{i \in I} \sum_{a \in \Gamma} \left(t_{i,a} \cdot \prod_{a' \in \Gamma \setminus \{a\}} \neg t_{i,a'} \right) \\
\varphi_{\delta} &:= s_{q_{\text{acc}}} + \neg s_{q_{\text{rej}}} \cdot \prod_{\substack{q \in Q_{\exists} \\ a \in \Gamma \\ i \in I}} \left((s_q \cdot p_i \cdot t_{i,a}) \rightarrow \sum_{\substack{(q', i, i+X, a') \\ (q', a', X) \in \delta(q, a)}} \varphi_{\text{next}}^{(q', i, i+X, a')} \right) \\
&\quad \prod_{\substack{q \in Q_{\forall} \\ a \in \Gamma \\ i \in I}} \left((s_q \cdot p_i \cdot t_{i,a}) \rightarrow \prod_{\substack{(q', i, i+X, a') \\ (q', a', X) \in \delta(q, a)}} \varphi_{\text{next}}^{(q', i, i+X, a')} \right) \\
\varphi_{\text{next}}^{(q', i, i', a')} &:= \text{EX}(s_{q'} \cdot p_{i'} \cdot t_{i, a'}) \cdot \prod_{\substack{j \in I \\ j \neq i \\ a \in \Gamma}} ((t_{j,a} \rightarrow \text{AX} t_{j,a}) \cdot (\neg t_{j,a} \rightarrow \text{AX} \neg t_{j,a}))
\end{aligned}$$

φ_{init} fixes the root of models of φ to simulate the initial configuration of M on x . $\text{AG}\varphi_{\text{conf}}$ enforces every reachable world to assume exactly one configuration of M . $\text{AG}\varphi_{\delta}$ requires the existence of successor configurations resulting from δ -transitions (and is falsified if q is the rejecting state), and finally $\varphi_{\text{next}}^{(q', i, i', a')}$ fixes all tape symbols at positions where the head currently does not write. Now it holds that φ is satisfiable if and only if the initial configuration of M is accepting. At this point it is crucial that all computation paths of M eventually accept or reject. This allows a correct reduction even without “eventuality” operators.

Case 2: AG, AF

The problem without AX is that it cannot be so easily modeled that the worlds quantified inside $\varphi_{\text{next}}^{(q', i, i', a')}$ coincide. Obviously it will not work to just replace AX, EX with AF, EF . Instead we do not quantify successors, but whole infinite paths which each assume a single reachable configuration and must eventually continue the computation.

$$\begin{aligned}
\varphi_{\text{next}}^{(q', i, i', a')} &:= \text{EG} \left[\prod_{\substack{j \in I \\ j \neq i \\ a \in \Gamma}} \underline{\varphi_{\text{keep}}^{(j,a)}} \cdot \left(\underline{(q', i', a')} \rightarrow (s_{q'} \cdot p_{i'} \cdot t_{i, a'}) \right) \right] \wedge \text{AF}(\underline{q', i', a'}) \\
\varphi_{\text{keep}}^{(j,a)} &:= (\text{AF}(b \cdot t_{j,a}) \rightarrow (t_{j,a} \cdot \text{AF}(\neg b \cdot t_{j,a}))) \cdot \\
&\quad (\text{AF}(\neg b \cdot t_{j,a}) \rightarrow (t_{j,a} \cdot \text{AF}(b \cdot t_{j,a}))) \\
\varphi &:= \varphi_{\text{init}} \cdot \text{AG}\varphi_{\text{conf}} \cdot \text{AG}\varphi_{\delta} \cdot \text{AG} \prod_{\substack{j \in I \\ a \in \Gamma}} \left(\underline{\varphi_{\text{keep}}^{(j,a)}} \rightarrow \varphi_{\text{keep}}^{(j,a)} \right)
\end{aligned}$$

Here, the underlined formulas are meant as atomic propositions. The formula $\varphi_{\text{keep}}^{(j,a)}$ is not directly inserted so we can retain a low temporal depth, and φ ensures with AG that the resulting formula is still correct.

Let π be a path that fulfills $\varphi_{\text{keep}}^{(j,a)}$. Then $\pi \models t_{j,a} \rightarrow \text{G}t_{j,a}$. Proof by induction over the length ℓ of a prefix of π . The case $\ell = 1$ is clear. For $\ell > 1$ assume w.l.o.g. that $\pi[\ell] \models b, t_{j,a}$. Then $\pi[\ell]$ must fulfill $\text{AF}(\neg b \cdot t_{j,a})$ but $\neg b$ cannot hold in $\pi[\ell]$ itself. Then by definition of AF the world $\pi[\ell + 1]$ must fulfill $\text{AF}[\neg b \cdot t_{j,a}]$ and therefore $t_{j,a}$ holds due to the implication.

The modified $\varphi_{\text{next}}^{(q', i, i', a')}$ eventually enforces a reachable world w to assume a successor configuration. All tape symbols at position $j \neq i$ remain unchanged. Then the computation continues from w on fresh paths starting at w (where then all tape symbols at positions except i' are fixed).

Case 3: AU

The idea is to further modify the approach in the previous case. To replace AG we use the fact that the computation tree has only to be verified until a point where q_{acc} or q_{rej} is legally reached. Therefore introduce a new proposition h (*halted*) and replace every $\text{AG}\psi$ by $\text{A}[\psi \text{U} h]$. Replace $\text{AF}(q', i', a')$ by $\text{A}[\neg h \text{U} \neg h \cdot (q', i', a')]$, every other $\text{AF}\psi$ by $\text{A}[\top \text{U} \psi]$, and $\text{EG}\psi$ by $\neg \text{A}[\top \text{U} \neg \psi]$. This ensures that $\neg h$ holds as long as the computation is continued; but also allows that the paths not usable for further computation (as they fixed all tape symbols but one) can label h after labeling (q', i', a') .

Case 4: AR

As $\text{AG}\psi \equiv \text{A}[\perp \text{R} \psi]$ we can use the AG, AX case and only have to modify $\varphi_{\text{next}}^{(q', i, i', a')}$.

$$\begin{aligned} \varphi_{\text{next}}^{(q', i, i', a')} := & \prod_{\substack{q \in Q \\ a \in \Gamma}} (s_q \cdot p_i \cdot t_{i,a} \rightarrow \text{E}[(s_q \cdot p_i \cdot t_{i,a}) \text{U} (s_{q'} \cdot p_{i'} \cdot t_{i,a'})]) \\ & \cdot \prod_{\substack{j \in I \\ i \neq j \\ c \in \Gamma}} (t_{j,c} \rightarrow \text{A}[\neg(s_q \cdot p_i \cdot t_{i,a}) \text{R} t_{j,c}]) \end{aligned}$$

The formula $\varphi_{\text{next}}^{(q', i, i', a')}$ requires a reachable world where eventually $s_{q'} \cdot p_{i'} \cdot t_{i,a'}$ holds. The AR subformulas state f.a. $j \neq i$ that $\neg(s_q \cdot p_i \cdot t_{i,a})$ releases $t_{j,c}$, i.e., the earliest world where $t_{j,c}$ has no longer to hold is exactly the world *after* where the EU is fulfilled (one of q , i or t_i must change in the transition, otherwise the machine would not halt).

◀

► **Theorem 3.19.** $\mathcal{B}_k(T)$ and $\mathcal{B}(T)$ have optimal model depth $2^{\Theta(n)}$ for all $k \geq 2$ if $\text{AU} \in T$, $\text{AR} \in T$, $\{\text{AG}, \text{AX}\} \subseteq T$ or $\{\text{AG}, \text{AF}\} \subseteq T$.

Proof. The upper bound is inherited from full CTL again (see Theorem 2.9), the lower bound for fragments containing AU or AF follows from Corollary 3.5 as AU can define AF with constant blow-up. We have to show the lower bound for AR and $\{\text{AG}, \text{AX}\}$.

On R -generable frames, the fragment $\mathcal{B}(\{\text{AG}, \text{AX}\})$ is equivalent to the modal logic KD with the *universal modality* \boxtimes . This logic can enforce a model of depth 2^n with a formula of size $\mathcal{O}(n^2)$ via a construction of a binary counter [Grä07]. We optimize the approach with a few extra propositions to obtain a formula which does the same but has only linear length.

$$\begin{aligned} \alpha := & (p_0 \leftrightarrow \text{carry}_{\leq 0}) \cdot \prod_{i=1}^n (p_i \cdot \text{carry}_{\leq i-1} \leftrightarrow \text{carry}_{\leq i}) \cdot \\ & (\text{reset}_{\leq 0} \rightarrow \neg p_0) \cdot \prod_{i=1}^n (\text{reset}_{\leq i} \rightarrow \neg p_i \cdot \text{reset}_{\leq i-1}) \cdot \\ & \prod_{i=1}^n (\text{store}_{\geq i-1} \rightarrow \text{store}_{i-1} \cdot \text{store}_{\geq i}), \\ \beta := & \prod_{i=1}^n (\text{store}_i \rightarrow (p_i \rightarrow \text{AX} p_i) \cdot (\neg p_i \rightarrow \text{AX} \neg p_i)) \end{aligned}$$

$$\begin{aligned}\gamma &:= \prod_{i=1}^n ((\text{carry}_{\leq i-1} \cdot \neg p_i) \rightarrow \text{AX}(p_i \wedge \text{reset}_{\leq i-1}) \cdot \text{store}_{\geq i+1}) \\ &\quad \cdot (\neg p_0 \rightarrow \text{AX} p_0 \cdot \text{store}_{\geq 1}) \\ \varphi &:= \text{AG}(\alpha \cdot \beta \cdot \gamma) \cdot \prod_{i=0}^n \neg p_i\end{aligned}$$

The idea is the same as in [Grä07]: The propositions p_i form a binary counter of length n which assumes the values $0 \dots 2^n - 1$ in this order. The value 0 is assumed in the root of the model. If the propositions in a world w form the counter value k , they are forced to form $k + 1$ in every successor world of w . This is done by the subformula γ : Search for the least significant bit with value 0 which has only 1s to the right. Force it to flip in the next world, but also flip all the bits to the right to 0. The higher significant bits may not change between w and its successor which is ensured by β and γ . The use of the formula α saves some big conjunctions and improves the formula length from $\mathcal{O}(n^2)$ to $\mathcal{O}(n)$.

When using AR we can define AG and EU but not AX, therefore some more work is required. We have to distinguish two cases: Whether the counter value changes from even to odd, i.e., the only changing bit is p_0 and it changes from zero to one, or it changes from odd to even, i.e., p_0 flips from one to zero.

In γ , replace $\text{AX}(p_i \cdot \text{reset}_{\leq i-1})$ by $\text{E}[p_0 \text{U}(p_i \cdot \text{reset}_{\leq i-1})]$ (the odd-to-even case) and $\text{AX} p_0$ by $\text{E}[\neg p_0 \text{U} p_0]$ (the even-to-odd case). This formula flips the correct bit p_i from zero to one as well as lesser significant bits from one to zero in some reachable world which is however not necessarily a direct successor. To retain the values of more significant bits until this world is actually reached, change β to:

$$\begin{aligned}\beta &:= \prod_{i=1}^n \left(\text{store}_i \rightarrow \left(p_0 \rightarrow (p_i \rightarrow \text{A}[\neg p_0 \text{R } p_i]) \right. \right. \\ &\quad \cdot (\neg p_i \rightarrow \text{A}[\neg p_0 \text{R } \neg p_i]) \Big) \\ &\quad \cdot \left(\neg p_0 \rightarrow (p_i \rightarrow \text{A}[p_0 \text{R } p_i]) \right. \\ &\quad \cdot (\neg p_i \rightarrow \text{A}[p_0 \text{R } \neg p_i]) \Big) \Big)\end{aligned}$$

This formula says that on all paths p_i resp. $\neg p_i$ must be kept if p_i should be stored until the first occurrence of p_0 resp. $\neg p_0$ (depending on whether the counter was odd or even). But the EU subformulas of γ are chosen exactly such that the negation of the releasing literal of p_0 is kept on the witnessing path until the point of fulfillment. Therefore all bits of higher significance are retained until this world, and altogether there is a simple path which assumes all the counter values $0 \dots 2^n - 1$ at least once. ◀

4 Flat CTL

The previous section has established complexity results and model size and depth lower bounds for temporal operator depth of at least two. This section on the other hand investigates the corresponding fragments of *flat* CTL, i.e., temporal depth one.

Define the function $w: \mathbb{R} \rightarrow \mathbb{R}$ as $w(x) := \frac{x}{W(x)}$ where $W(x)$ is the Lambert W function restricted to real numbers (cf. [Cor+96]).

► **Lemma 4.1.** $w(x \ln x) = x$.

► **Theorem 4.2.** $\mathcal{B}_1(T)$ has optimal model size $w(\Theta(n))$ and depth 1 if T is $\{AX\}$ or $\{AG\}$, resp. depth 2 if T is $\{AX, AG\}$.

Proof. First we show the upper bound. Let φ be a flat CTL formula and w.l.o.g. in negation normal form. It then has the form $f(E\gamma_1, \dots, E\gamma_n, A\alpha_1, \dots, A\alpha_m)$, where f is a (negation-free) Boolean function and the γ, α are single temporal operators enclosing only propositional formulas. If φ is satisfiable, then it has a model where each $E\gamma$ is satisfied on its own path together with every $A\alpha$. It holds that each EF and EX require only a single world in the model and AG and AX cannot asymptotically influence the number of worlds.

Assume that a formula enforces m distinct worlds using EF. Then the m eventualities have to be pairwise inconsistent, i.e., for each pair (ψ, ψ') of eventualities they have to assign at least one propositional variable p_i complementary (we can assume that they use only \wedge, p_i and $\neg p_i$). What is the sum over all lengths of this eventualities? In fact this problem is equivalent to the *biclique covering* problem: Consider the m -clique graph K_m with the eventualities ψ_1, \dots, ψ_m as vertices. The goal is to cover all edges, where a covered edge (ψ, ψ') in K_m means that ψ and ψ' are inconsistent. To cover an edge we have to add a propositional variable first to ψ and then negated to ψ' . Generally, each propositional variable p is added to some eventualities (the A set) and $\neg p$ to others (the B set). Every $\psi \in A$ then contradicts each $\psi' \in B$: The covered edges form a biclique $A \times B$, and any such added biclique covers $|A| \cdot |B|$ edges in K_m . Likewise $|A| + |B|$ is the *weight* of the biclique, the number of literals added to the formula. Now the *minimal weight biclique covering* has at most weight $h(m)$ (where $h(m) \leq \lceil m \log m \rceil$ is the binary entropy) and at least weight $m \log m$ [Juk11, p. 46]. This translates to a required formula size of $m \log m$, and conversely to at most m worlds required to fulfill a flat formula of length $m \log m$. This argumentation holds for EF and EX. Hence in the case that only AX, EX, AG and EF are available, a flat formula of size $m \log m$ can only enforce a model of size up to m and a depth of at most two (when EF is pushed to depth two by AX) resp. one (if not both EF and AX are available).

For the lower bound consider the formula family $\varphi_m := \prod_{i=0}^{m-1} EF\vec{c}_i$, where the \vec{c}_i are conjunctions of size $\lceil \log m \rceil$ representing the value i as a binary vector. These formulas are satisfiable. For some constant d and large enough m it is $|\varphi_m| \leq d m \log m$, but φ_m has only models with size at least $m = w(m \log m) \geq w(\frac{|\varphi_m|}{d})$ for some d (w is monotone). For EX instead of EF the formula works analogously. ◀

► **Theorem 4.3.** $\mathcal{B}_1(T)$ has optimal model size $w(\Theta(n))^2$ and depth $w(\Theta(n))$ if $AF \in T$ and $T \subseteq \{AX, AG, AF\}$.

Proof. We extend the proof of the last theorem and now assume that only EG and AF are available. We can assume this since the worst case is that all eventualities are bound to A quantifiers and invariants to E quantifiers.

The maximal model size is reached when the AFs pairwise contradict and when the paths fulfilling the EGs have only their root world in common. As the paths have to fulfill the same eventualities, they can only be prevented from joining if the k EGs again have size $k \log k$ together. It follows that a satisfiable formula with m AFs and k EGs can enforce a model of size up to $\mathcal{O}(m \cdot k)$ with length $m \log m + k \log k$. For a fixed formula length $2c$ we assume $c + \delta$ as length of the AF formulas and $c - \delta$ as length of the EG formulas. The enforced model size is then at most $w(c + \delta) \cdot w(c - \delta)$ which is maximal for $\delta = 0$.

For the lower bound consider the formula $\vec{c}_0 \cdot \prod_{i=0}^{m-1} AF\vec{c}_i \cdot \prod_{i=0}^{m-1} EG(\vec{c}_0 + \vec{d}_i)$, where \vec{c}_i and \vec{d}_i are again binary vectors of size $\lceil \log m \rceil$ representing the value i .

Then the EGs can only be fulfilled on m paths for which holds that every common world must have labeled \vec{c}_0 . But as every path must have labeled $\vec{c}_1, \dots, \vec{c}_{m-1}$ somewhere, each

path owns at least $m - 2$ worlds which do not belong to any other path. It follows that the formula is satisfiable, has size $\mathcal{O}(m \log m)$, but no model smaller than m^2 or shallower than depth m . ◀

► **Theorem 4.4.** $\mathcal{B}_1(T)$ has optimal model size $\Theta(n) \cdot w(\Theta(n))$ and depth $\Theta(n)$ if T contains AU or AR.

Proof. First assume the case that AU or equivalently ER is available. For the depth lower bound use the formula $\prod_{i=0}^{m-1} A[\neg p_i U p_{i-1}]$.

Using ERs of total length $k \log k$ allows an additional factor k in the model size similar to EG in the previous theorem. Then such a formula has length $\mathcal{O}(m + k \log k)$ and models of size at least $\Omega(m \cdot k)$. Set $m := \lceil k \log k + k \rceil$, then there is a formula family with length $\mathcal{O}(k \log k)$ and model size at least $k^2 \log k$.

For the case with AR or equivalently EU the bounds for the optimal depth stay the same. For the size lower bound it is required that the EUs branch on distinct paths and are not fulfilled before the last AR is fulfilled on every path: Use for instance $\prod_{i=0}^{k-1} E[(p_0 + \vec{c}_i) U h]$ and $\prod_{i=0}^{m-1} A[(\neg h \cdot p_i) R (\neg h \cdot \neg p_{i+1})]$, where the EUs are separated by the bit vectors \vec{c}_i . In this formula the ARs have to be fulfilled in ascending order and before the EUs are fulfilled.

The upper bound for the depth of \mathcal{B}_1 is linear even for the full set of CTL operators. For the size we neglect X and assume that all other operators are rewritten to AU, EU, AR and ER. Then every satisfiable formula with length $k \log k$ has a model of size $\mathcal{O}(k^2 \log k)$: $k \log k$ symbols can contain only up to k ERs resp. EUs enforcing distinct paths, or up to $k \log k$ AUs resp. ARs enforcing $k \log k$ points of fulfillments on all paths, and both always fits in a model of size $\mathcal{O}(k^2 \log k)$. ◀

5 Restricted Boolean clones

Post's lattice of Boolean clones enormously helps to study the different nature of Boolean functions. Regarding the specific problem of propositional satisfiability it was shown by Lewis that the clones containing S_1 are NP-hard, while the problem restricted to arbitrary other clones is tractable [Lew79].

The Boolean clone S_1 is the clone of *1-separating* functions. A function $f(b_1, \dots, b_n)$ is 1-separating if it has one argument b_i that is always one if f is one; or equivalently if it can be expressed using only the negated implication \rightarrow . In this section we show that the same dichotomy as for propositional satisfiability holds for CTL in the sense that all lower bounds can be carried over to S_1 .

► **Lemma 5.1.** Let $(\varphi_n)_{n \in \mathbb{N}}$ be a family of satisfiable $\mathcal{B}_k(T)$ formulas for some $k \in \mathbb{N}$, $T \subseteq \text{TL}$. Let φ_n have minimal model size $s(n)$ and minimal model depth $d(n)$.

Let C be a finite set of Boolean functions s. t. $S_1 \subseteq [C]$. Then there is a family $(\varphi'_n)_{n \in \mathbb{N}}$ of satisfiable $\mathcal{B}_k(C, T)$ formulas with minimal model size $s(n)$ resp. depth $d(n)$ s. t. φ'_n has size $\mathcal{O}(|\varphi_n|)$.

Proof. For each φ_n define a formula φ'_n which uses only operators from C . It is $[S_1 \cup \{\top\}] = \text{BF}$ [Pos41]. Hence the occurrences of \wedge, \vee, \neg in φ can be rewritten using symbols from C and \top , increasing formula size only by a constant factor due to *short representations* [Lew79]. Then to obtain φ'_n replace \top by a fresh variable t and append $\wedge t$ to every subformula which is directly under the scope of a temporal operator. Then it holds: Every model of φ_n is a model of φ'_n when t is added to every world, and vice versa every model of φ'_n is a model of φ_n . It remains to show that $\wedge t$ can be added without too large overhead. $\wedge \in S_1$, yet it does

not necessarily have a short representation with symbols from C . But as the temporal depth is at most k , the formula size increases at most by e^k where e is some constant depending on C . ◀

The transformation given in the last proof is in fact a polynomial time reduction:

► **Corollary 5.2.** *Let C be a finite set of Boolean functions s. t. $S_1 \subseteq [C]$. For all k it holds $\text{SAT}(\mathcal{B}_k(T)) \leq_m^P \text{SAT}(\mathcal{B}_k(C, T))$.*

Therefore all shown lower bounds which hold for formulas of constant temporal depth already hold for any Boolean function set C which can express S_1 .

The only remaining case which was not a result for constant temporal depth is **AX**.

► **Theorem 5.3.** *Let C be a finite set of Boolean functions such that $S_1 \subseteq [C]$. Then $\text{SAT}(\mathcal{B}(C, \{\text{AX}\}))$ is \leq_m^P -complete for **PSPACE**.*

Proof. We proceed similar to Lemma 5.1, but we cannot so easily enforce t being labeled in any world of a potential model. Instead we make use of the upper bound for model depth shown in Theorem 3.12 and transform $\varphi \in \mathcal{B}(\text{AX})$ to $\varphi \cdot \prod_{i=0}^k \Box^i t$, where k is the temporal depth of φ .

\wedge is associative, therefore the k new conjuncts can be rewritten to an expression with parenthesis nesting depth of $\lceil \log k \rceil$. As the rewriting of \wedge to symbols of C leads to a constant blow-up on each of the $\lceil \log k \rceil$ levels, the whole blow-up is $c^{\lceil \log k \rceil} \in |\varphi|^{\mathcal{O}(1)}$, so the reduction runs in polynomial time. ◀

6 Summary and conclusion

Results.

The results are summarized in the following theorems.

► **Theorem 6.1.** *Let C be a finite set of Boolean functions such that $S_1 \subseteq [C]$, and let T be a non-empty set of temporal operators. Then $\text{SAT}(\mathcal{B}(C, T))$ is*

- **PSPACE**-complete if **AX** can define T ,
- equivalent to $\text{SAT}(\mathcal{B}_2(C, T))$ otherwise, and therefore
 - **PSPACE**-complete if T can be defined by $\{\text{AX}, \text{AF}\}$ or **AG**,
 - **EXP**-complete otherwise.

Proof. The first case was shown in Theorem 5.3. All other cases follow from Corollary 5.2 together with the hardness results from Theorem 3.4 and 3.17 for **AF** (and **AX**), from Theorem 3.6 and 3.7 for **AG**, and from Theorem 3.18 and 2.10 for the other operators. ◀

► **Theorem 6.2.** *Let C be a finite set of Boolean functions such that $S_1 \subseteq [C]$. Then the satisfiability problem $\text{SAT}(\mathcal{B}_1(C, T))$, i.e., for flat CTL, is **NP**-complete under \leq_m^P -reduction for any operator set $T \subseteq \text{TL}$.*

Proof. See Theorem 3.13 and Corollary 5.2. The polynomial model property follows from Theorem 4.2 and Theorem 4.4. ◀

The NP membership for flat CTL is not only of purely theoretical relevance. In principle it is possible to tackle the problem with a SAT solver; the key idea is here to decompose the formula in multiple SAT instances. Every **AF** must be consistent with every **EG**, but not necessarily with each other, **AG** must be consistent with any other subformula, the **AU**

T	\mathcal{B}_1	$\mathcal{B}_{k \geq 2}$	\mathcal{B}
AX	NP-c.	NP-c.	PSPACE-c.
AF	NP-c.	PSPACE-c.	PSPACE-c.
AG	NP-c.	PSPACE-c.	PSPACE-c.
AF, AX	NP-c.	PSPACE-c.	PSPACE-c.
AG, AX	NP-c.	EXP-c.	EXP-c.
AG, AF	NP-c.	EXP-c.	EXP-c.
AU, *	NP-c.	EXP-c.	EXP-c.
AR, *	NP-c.	EXP-c.	EXP-c.

■ **Figure 1** Complexity of $\text{SAT}(\mathcal{B}(T))$

T	$\sigma(\mathcal{B}_1)$	$\delta(\mathcal{B}_1)$	$\sigma(\mathcal{B}_{k \geq 2})$	$\delta(\mathcal{B}_{k \geq 2})$	$\sigma(\mathcal{B})$	$\delta(\mathcal{B})$
AX	$w(n)$	1	$n^{\Theta(1)}$	$\Theta(1)$	$2^{\Omega(\sqrt{n})} \cap 2^{\mathcal{O}(n)}$	n
AF	$w(n)^2$	$w(n)$	2^n	2^n	2^n	2^n
AG	$w(n)$	1	2^n	n	2^n	n
AF, AX	$w(n)^2$	$w(n)$	2^n	2^n	2^n	2^n
AG, AX	$w(n)$	2	2^n	2^n	2^n	2^n
AG, AF	$w(n)^2$	$w(n)$	2^n	2^n	2^n	2^n
AU, *	$n \cdot w(n)$	n	2^n	2^n	2^n	2^n
AR, *	$n \cdot w(n)$	n	2^n	2^n	2^n	2^n

○ sublinear ○ polynomial ○ superpolynomial

■ **Figure 2** Optimal model size σ and depth δ of $\text{SAT}(\mathcal{B}(T))$, $n = \Theta(|\varphi|)$

require consistency along some ordering between them, but they can all be satisfied on a path before the AFs, and so on. Likewise it is obvious why this approach cannot work with multiple nested temporal operators.

► **Theorem 6.3.** *Let C be a finite set of Boolean functions such that $S_1 \subseteq [C]$, and let T be a non-empty set of temporal operators. Then it holds for $k \geq 2$, $\sigma = \sigma(\mathcal{B}(C, T))$, $\delta = \delta(\mathcal{B}(C, T))$, $\sigma_k = \sigma(\mathcal{B}_k(C, T))$ and $\delta_k = \delta(\mathcal{B}_k(C, T))$:*

- $\sigma \in 2^{\Omega(\sqrt{n})} \cap 2^{\mathcal{O}(n)}$, $\sigma_k \in n^{\Theta(1)}$, $\delta \in \Theta(n)$, $\delta_k \in \Theta(1)$ if AX can define T ,
- $\sigma, \sigma_k \in 2^{\Theta(n)}$ otherwise.
- $\delta, \delta_k \in \Theta(n)$ if AG can define T ,
- $\delta, \delta_k \in 2^{\Theta(n)}$ if neither AG nor AX can define T .
- $\sigma_1 \in w(\Theta(n))$, $\delta_1 = 2$ if $\{\text{AG}, \text{AX}\}$ is equivalent to T ,
- $\sigma_1 \in w(\Theta(n))$, $\delta_1 = 1$ if $\{\text{AG}, \text{AX}\}$ can define T but not vice versa,
- $\sigma_1 \in w(\Theta(n))^2$ if T can define AF but neither AU nor AR,
- $\sigma_1 \in \Theta(n) \cdot w(\Theta(n))$ if T can define AU or AR.

Proof. The non-flat cases follow from the combination of Corollary 3.5, 3.11, 3.12 and 3.19 with Lemma 5.1. The cases for flat CTL are again proven by Lemma 5.1 together with Theorem 4.2, 4.3 and 4.4. ◀

Conclusion.

The results show an interesting property of the computation tree logic CTL: The computational complexity abruptly jumps between temporal depth one and two, if we leave aside the pure modal fragment. The flat fragments are all in NP, and could in fact be solved by common SAT-solvers in practice. But if a nesting depth of two is allowed, then already the complexity of full CTL emerges which lies between PSPACE- and EXP-completeness. This is reasonable if AG is available, as we then simply can “pull out” too deeply nested subformulas until a temporal depth of only two, but for the other fragments this is still an interesting result. From the viewpoint of practical application this paper is clearly a negative result as many important properties of transition systems are modeled as \mathcal{B}_2 - or \mathcal{B}_3 -formulas. Yet it is very interesting that not only the hardness results in terms of computational complexity can be carried over to \mathcal{B}_2 , but also the lower bounds for optimal model size and depth. Furthermore on the level of Boolean functions, just as for propositional logic, it suffices any set expressing the 1-separating functions to establish all presented lower bounds.

When comparing the results to a preceding study for the linear temporal logic LTL [DS02], one finds many (possibly expected) similarities. All fragments of flat LTL are NP-complete which should not surprise at this point. LTL falls down to NP also when restricted to only X, F or G; exponentially long paths cannot be enforced in these cases [SC85]. Here the power of branching gives an advantage to CTL regarding such long paths. On the other hand the PSPACE-complete fragments of LTL satisfiability, namely U and {F, G, X}, correspond to the EXP-complete CTL cases AU, {AG, AX} and {AG, AF}. Moreover the results for CTL and LTL match very nicely in the sense that (i) for both logics the bounded X-case is NP-complete and (ii) the lower bounds for all other operators already hold for temporal depth of two.

In future research it would be interesting to possibly expand this principle to similar logics and show similar tight lower bounds. Candidates would be CTL^+ which allows arbitrary Boolean combinations of flat path formulas in the scope of a path quantifier, of course the full branching time logic CTL^* [AEH86], and the fairness extension of CTL with the operators $\overset{\infty}{F} := GF$ and $\overset{\infty}{G} := FG$ inside the path quantifiers.

Acknowledgments

This work was developed in collaboration with the DFG project ME 4279/1-1.

The author thanks Anselm Haak, Fabian Müller, Arne Meier and Heribert Vollmer from the Institute for Theoretical Computer Science in Hannover for their many useful critical comments and hints.

References

- [AE90] E. Allen Emerson. *Temporal and Modal Logic*. Handbook of Theoretical Computer Science (Vol. B). Ed. by J. van Leeuwen. Cambridge, MA, USA: MIT Press, 1990, pp. 995–1072.
- [AEH85] E. Allen Emerson, J. Y. Halpern. *Decision procedures and expressiveness in the temporal logic of branching time*. Journal of Computer and System Sciences **30** (Feb. 1985), no. 1, pp. 1–24. DOI: [10.1016/0022-0000\(85\)90001-7](https://doi.org/10.1016/0022-0000(85)90001-7).
- [AEH86] E. Allen Emerson, J. Y. Halpern. “Sometimes” and “Not Never” Revisited: On Branching Versus Linear Time Temporal Logic. J. ACM **33** (Jan. 1986), no. 1, pp. 151–178. DOI: [10.1145/4904.4999](https://doi.org/10.1145/4904.4999).

- [Bey+09] O. Beyersdorff, A. Meier, M. Mundhenk, M. Thomas, T. Schneider, H. Vollmer. *Model Checking CTL is Almost Always Inherently Sequential*. Temporal Representation and Reasoning, 2009. TIME 2009. 16th International Symposium on. July 2009, pp. 21–28. DOI: [10.1109/TIME.2009.12](https://doi.org/10.1109/TIME.2009.12).
- [CAES86] E. M. Clarke, E. Allen Emerson, A. P. Sistla. *Automatic verification of finite-state concurrent systems using temporal logic specifications*. ACM Transactions on Programming Languages and Systems (TOPLAS) **8** (1986), no. 2, pp. 244–263.
- [CKS81] A. K. Chandra, D. C. Kozen, L. J. Stockmeyer. *Alternation*. J. ACM **28** (Jan. 1981), no. 1, pp. 114–133. DOI: [10.1145/322234.322243](https://doi.org/10.1145/322234.322243).
- [Coo71] S. A. Cook. *The complexity of theorem-proving procedures*. ACM Press, 1971, pp. 151–158. DOI: [10.1145/800157.805047](https://doi.org/10.1145/800157.805047).
- [Cor+96] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, D. E. Knuth. *On the Lambert W function*. Advances in Computational Mathematics **5** (1996), no. 1, pp. 329–359. DOI: [10.1007/BF02124750](https://doi.org/10.1007/BF02124750).
- [DS02] S. Demri, P. Schnoebelen. *The Complexity of Propositional Linear Temporal Logics in Simple Cases*. Information and Computation **174** (2002), no. 1, pp. 84–103. DOI: [10.1006/inco.2001.3094](https://doi.org/10.1006/inco.2001.3094).
- [FL79] M. J. Fischer, R. E. Ladner. *Propositional dynamic logic of regular programs*. Journal of Computer and System Sciences **18** (1979), no. 2, pp. 194–211. DOI: [http://dx.doi.org/10.1016/0022-0000\(79\)90046-1](http://dx.doi.org/10.1016/0022-0000(79)90046-1).
- [Grä07] E. Grädel, ed. *Finite model theory and its applications*. Texts in theoretical computer science. Berlin ; New York: Springer, 2007.
- [Hal95] J. Y. Halpern. *The Effect Of Bounding The Number Of Primitive Propositions And The Depth Of Nesting On The Complexity Of Modal Logic*. Artificial Intelligence **75** (1995), pp. 361–372.
- [Juk11] S. Jukna. *Extremal Combinatorics: With Applications in Computer Science*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2011.
- [Lad77] R. E. Ladner. *The Computational Complexity of Provability in Systems of Modal Propositional Logic*. SIAM Journal on Computing **6** (1977), no. 3, pp. 467–480. DOI: [10.1137/0206033](https://doi.org/10.1137/0206033).
- [Lew79] H. R. Lewis. *Satisfiability problems for propositional calculi*. English. Mathematical systems theory **13** (1979), no. 1, pp. 45–53. DOI: [10.1007/BF01744287](https://doi.org/10.1007/BF01744287).
- [Mar07] M. Marx. *3 Complexity of modal logic*. Handbook of Modal Logic. Ed. by J. V. B. Patrick Blackburn, F. Wolter. **3**. Studies in Logic and Practical Reasoning. Elsevier, 2007, pp. 139–179. DOI: [http://dx.doi.org/10.1016/S1570-2464\(07\)80006-1](http://dx.doi.org/10.1016/S1570-2464(07)80006-1).
- [MMTV09] A. Meier, M. Mundhenk, M. Thomas, H. Vollmer. *The complexity of satisfiability for fragments of CTL and CTL**. International Journal of Foundations of Computer Science **20** (2009), no. 05, pp. 901–918.
- [MS73] A. R. Meyer, L. J. Stockmeyer. *Word problems requiring exponential time (Preliminary Report)*. ACM Press, 1973, pp. 1–9. DOI: [10.1145/800125.804029](https://doi.org/10.1145/800125.804029).
- [Pnu77] A. Pnueli. *The temporal logic of programs*. Foundations of Computer Science, 18th IEEE Annual Symposium on. 1977, pp. 46–57. DOI: [10.1109/SFCS.1977.32](https://doi.org/10.1109/SFCS.1977.32).
- [Pos41] E. L. Post. *On The Two-Valued Iterative Systems of Mathematical Logic*. Princeton University Press, 1941.

- [Pra80] V. R. Pratt. *A near-optimal method for reasoning about action*. Journal of Computer and System Sciences **20** (1980), no. 2, pp. 231–254. DOI: [http://dx.doi.org/10.1016/0022-0000\(80\)90061-6](http://dx.doi.org/10.1016/0022-0000(80)90061-6).
- [Pri57] A. N. Prior. *Time and Modality*. Oxford, 1957.
- [SC85] A. P. Sistla, E. M. Clarke. *The Complexity of Propositional Linear Temporal Logics*. Journal of the ACM **32** (1985), no. 3, pp. 733–749.
- [Sch02] P. Schnoebelen. *The Complexity of Temporal Logic Model Checking*. Advances in Modal Logic. Ed. by P. Balbiani, N.-Y. Suzuki, F. Wolter, M. Zakharyashev. King's College Publications, 2002, pp. 393–436.